using said first ~~an~~ encrypt and decrypt engine for encrypting and decrypting data with a private key ~~using associative properties of encrypting and decrypting~~, wherein said encrypt and decrypt engine can encrypt an unsecured data file with a first private key into a first encrypted file~~;~~;

using a second encrypt and decrypt engine for encrypting the first encrypted data file with a second private key into a second encrypted file~~;~~;

using said first encrypt and decrypt engine for decrypting the second encrypted file with the first private key into a third encrypted file~~;~~; and

using said second encrypt and decrypt engine for decrypting the third encrypted file with the second private key into the unsecured data file.

2. (original) The system of claim 1, wherein the private keys contain biometric data identifying its user.

3. (currently amended) A method of encrypting, decrypting and transmitting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

providing unsecured data for transmission at the first computer;

downloading an encrypt and decrypt engine to said first computer over a computer network for encrypting and decrypting data;

encrypting the unsecured data using a first private key into a first encrypted data file;

transmitting the first encrypted data file to the second computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file;

transmitting the second encrypted data file to the first computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file;

transmitting the third encrypted data file to the second computer; and

decrypting the third encrypted data file using the second private key into the unsecured data.

4. (original) The method of claim 3, further including the step of storing the unsecured data on the second computer.

5. (original) The method of claim 3, further including the step of verifying the validity of the unsecured data after decrypting the third encrypted data file at the second computer.

6. (original) The method of claim 3, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.

7. (original) The method of claim 3, wherein the private keys can include digitized biometric data identifying its user.

8. (original) The method of claim 3, further including the step of processing the unsecured data after decrypting the third encrypted data file at the second computer.

9. (currently amended) A method of encrypting and decrypting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

downloading an encrypt and decrypt engine to said first computer over a computer network for encrypting and decrypting data;

encrypting unsecured data using a first private key into a first encrypted data file at the first computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file at the second computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file at the first computer; and

decrypting the third encrypted data file using the second private key into the unsecured data at the second computer.

10. (original) The method of claim 9, further including the step of storing the unsecured data on the second computer.

11. (original) The method of claim 9, further including the step of verifying the validity of the unsecured data after decrypting the third encrypted data file at the second computer.

12. (original) The method of claim 9, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.

13. (original) The method of claim 9, wherein the private keys can include digitized biometric data identifying its user.

14. (original) The method of claim 9, further including the step of processing the unsecured data after decrypting the third encrypted data file at the second computer.

15. (currently amended) A computer-readable medium comprising program instructions for encrypting and decrypting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

downloading an encrypt and decrypt engine to said first computer over a computer network for encrypting and decrypting data;

encrypting unsecured data using a first private key into a first encrypted data file at the first computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file at the second computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file at the first computer; and

decrypting the third encrypted data file using the second private key into the unsecured data at the second computer.

16. (original) The method of claim 15, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.